**SUMA DE CUADRADOS**

Nº inscripción :00/2000/3213

R.P.I- VA-2060

**CONDICIONES NECESARIAS Y SUFICIENTES PARA QUE UN NUMERO SEA SUMA DE DOS CUADRADOS**

---

No todo número puede ser representado como suma de dos cuadrados.

Pierre de Fermat (1601-1665) ,conocido como el padre de la Teoría de Números , en carta de 25 de diciembre de 1640 , dirigida a Marín Mersenne , fraile franciscano , enunció el teorema que afirmaba que un número primo de la forma $4n + 1$ , puede expresarse de una manera como suma de dos cuadrados. Añadía, que si un número primo, que es suma de dos cuadrados , se multiplica por otro primo que también es suma de dos cuadrados , el producto sería la suma de dos cuadrados , de dos formas distintas (1).

Fermat, también afirmó, que ningún número primo de la forma $4n+3$ puede expresarse como suma de dos cuadrados (1)

Existe una fórmula sencilla, ya usada por Diofanto :

$$(a^2 + b^2)(c^2 + d^2) = (ac+bd)^2 + (ad-bc)^2 = (ac-bd)^2 + (ad+bc)^2$$

que permite observar que el producto de dos números ,que son suma de dos cuadrados , es también suma de dos cuadrados.

Entre otros matemáticos que estudiaron este problema, podemos citar a Bachet, en sus comentarios al Libro de Diofanto, François Viète y Albert Girad ( 1595-1632). Este afirmaba , que un número es suma de dos cuadrados , si es un cuadrado, o es el 2 , o es 1 más múltiplo de 4 , o un producto de tales números. La parte difícil de este Teorema, es probar qué condiciones son suficientes. (2)

---

En nuestro estudio , hacemos referencia a todo número , N , entero , positivo, impar, no múltiplo de un cuadrado, ni múltiplo de 3 .

Pueden ser números primos o compuestos .

Los números múltiplos de cuadrado, se dividirán por estas cifras, tantas veces como lo permita el número, hasta obtener el número "N" , válido para el estudio.

Al final del estudio se tendrá en cuenta esta simplificación.

**$N = a^2 + b^2$ .-CONDICIONES NECESARIAS Y SUFICIENTES**

Como sabemos, la condición necesaria , pero no suficiente, es que :

$$N \equiv 1 \ (\text{módulo } 4) \ .$$

## T E O R E M A

Como condiciones necesarias y suficientes, citaré aquellas en las que se fundamenta mi Teorema , y que más adelante justifico :

A ) .- Para todo "N", suma de dos cuadrados , dado un resto cuadrático R , módulo el citado "N" , tiene que existir al menos otra pareja de cuadrados , que genere como resto (N-R).

B).- Para que "N" sea igual a la suma de 2 cuadrados, es preciso que "N" sea igual a la suma de dos cuadrados consecutivos , más dos veces el producto de 2 números consecutivos :

$$N = e^2 + (e+1)^2 + 2f\,(f+1)$$

C).- Que la suma de 4 cuadrados consecutivos , sea congruente la unidad , módulo "N" .

$$g^2 + (g+1)^2 + (g+2)^2 + (g+3)^2 \equiv 1 \ (\text{módulo } N)$$

Podemos citar 2 condiciones necesarias y suficientes , que tienen su fundamento en las arriba citadas :

D).- Igualmente será condición necesaria y suficientes que N + 1 sea igual a la suma de 4 cuadrados consecutivos más 16 veces el producto de dos determinados números consecutivos :

$$N+1 = \frac{(a-3)^2}{4} + \frac{(a-1)^2}{4} + \frac{(a+1)^2}{4} + \frac{(a+3)^2}{4} + 16\,t\,(t+1)$$

E).- Que la suma de 4 cuadrados consecutivos pares, sea congruente 16 , módulo N :

$$h^2 + (h+2)^2 + (h+4)^2 + (h+6)^2 = 16 \text{ ( módulo N )}$$

A continuación vamos a justificar el "por qué" ,de las citadas condiciones :

**JUSTIFICACION, CONDICION "A"**

Para todo "N" , suma de 2 cuadrados , dado un resto cuadrático R , módulo el citado "N" , tiene que existir al menos otra pareja de cuadrados que genere el resto N – R .

Creemos que esta condición está suficiente mente justificada, y con argumentos diversos.- Citaremos uno :

$N = a^2 + b^2$ $\qquad a^2 = R \qquad b^2 = N - R$

Otro cualquier resto cuadrático, $f^2 \equiv R(2)$ (módulo N ).- Teniendo en cuenta una de las propiedades de los restos cuadráticos, el producto de multiplicar dos restos cuadráticos ,genera otro resto. Luego tiene que existir un resto " r " ,que multiplicado por "R" , genere como resto "R(2)".

R . r ≡ R(2) ( módulo N ) .- Siendo esto así ,

$$(N - R) \cdot r \equiv [\, N - R(2) \,] \text{ ( módulo N )}$$

---

Conociendo el cuadrado que genera como resto N-1 , es fácil determinar cualquier cuadrado que genere como resto N – R .

Ejemplo : $N = 3.977 = a^2 + b^2 = 61^2 + 16^2 = 29^2 + 56^2$

$C^2 \equiv (N - 1)$ ( módulo N ) ; $\quad C = (d N - b) / a \qquad C = (3977\, d - 61) / 16$

Resolvemos la ecuación indeterminada

| 16 | |
|---|---|
| 9 | 1 |
| 3 | 11 |
| 1 | 9 |
| 61 | 5 |

d = 5 $\qquad$ C = 1.239

$1239^2 \equiv 3976$ ( módulo 3977 ) $\qquad K^2 \equiv R$ ( módulo N )

$$K^2 \cdot 1239^2 \equiv (N - R) \text{ ( módulo N )}$$

**JUSTIFICACION CONDICION " B "**

Esta hacía referencia a :

$$N = e^2 + (e+1)^2 + 2f(f+1)$$

$$N = a^2 + b^2 \qquad a > b\ ; \quad e = \frac{a+b-1}{2}\ ; \qquad f = a-e-1 = e-b$$

---

$$N = e^2 + (e+1)^2 + 2f(f+1) = \frac{(a+b+1)^2}{4} + \frac{(a+b-1)^2}{4} + \frac{(a-b)^2 - 1}{2}$$

Esto es fácilmente demostrable ,

$$\frac{(a+b+1)^2}{4} + \frac{(a+b-1)^2}{4} = \frac{(a+b)^2 + 1}{2}$$

La diferencia entre ,

$$a^2 + b^2 - \frac{(a+b)^2 + 1}{2} = \frac{(a-b)^2 - 1}{2}$$

y como quiera que ,

$$(a-b)^2 - 1 = (a-b+1)(a-b-1)$$

$\frac{(a-b)^2 - 1}{2}$ es igual al producto de multiplicar por 2 , dos números consecutivos.

Ejemplo : $N = 12.719.837 = 2348^2 + 2347^2 + (2 \times 921 \times 922)$

$$12.719.837 = (2348+921)^2 + (2347-921)^2 = 3269^2 + 1426^2$$

**JUSTIFICACION CONDICION " C "**

Esto hace referencia a :

$$g^2 + (g+1)^2 + (g+2)^2 + (g+3)^2 \equiv 1 \pmod{N}$$

$$g = \frac{N - 2C - 3}{2} \qquad C^2 \equiv (N-1) \pmod{N}$$

---

La justificación es muy simple :

$$g^2 = \frac{(g-3)^2}{4} + \frac{(g-1)^2}{4} + \frac{(g+1)^2}{4} + \frac{(g+3)^2}{4} - 5$$

Ejemplo : $359^2 = 178^2 + 179^2 + 180^2 + 181^2 - 5$

$$\frac{(g-3)^2}{4} + \frac{(g-1)^2}{4} + \frac{(g+1)^2}{4} + \frac{(g+3)^2}{4} - 5 = \frac{4g^2 + 20}{4} - 5 = g^2$$

Por otra parte , si consideramos que :

$$C^2 \equiv (N-1) \pmod{N} \qquad C^2 \equiv -1 \pmod{N}$$

$$(2C)^2 \equiv -4 \pmod{N} \qquad 2C \equiv 0 \pmod{2} \qquad (N - 2C) \text{ es impar}$$

$$\frac{(N-2C-3)^2}{4} + \frac{(N-2C-1)^2}{4} + \frac{(N-2C+1)^2}{4} + \frac{(N-2C+3)^2}{4} - 5 \equiv -4 \pmod{N}$$

la suma de los cuatro cuadrados es congruente más uno , módulo "N" .

**JUSTIFICACION CONDICION " E "**

Esta decía :

$$h^2 + (h+2)^2 + (h+4)^2 + (h+6)^2 \equiv 16 \ (\text{módulo } N)$$

$$h = C - 3$$

---

Si multiplicamos por 4 ,dos al cuadrado , la ecuación de la condición "C" , llegaríamos a :

$$(2g+6)^2 = g^2 + (g+2)^2 + (g+4)^2 + (g+6)^2 - 20$$

Ejemplo : $718^2 = 356^2 + 358^2 + 360^2 + 362^2 + 20$

para $(2g+6) \equiv 2 \ (\text{módulo } 4)$

Recordemos que tiene que existir un cuadrado :

$$(2g+6)^2 \equiv -4 \ (\text{módulo } N)$$

$$(2h+6)^2 = h^2 + (h+2)^2 + (h+4)^2 + (h+6)^2 - 20 \equiv -4 \ (\text{mód. } N)$$

luego , $h^2 + (h+2)^2 + (h+4)^2 + (h+6)^2 \equiv 16 \ (\text{mód. } N)$

Ejemplo :

$N = 3977 \qquad 1239^2 \equiv -1 \ (\text{mód.} 3977) ; \qquad 2478^2 \equiv -4 \ (\text{mód. } 3977)$

$$1236^2 + 1238^2 + 1240^2 + 1242^2 \equiv 16 \ (\text{módulo } 3977)$$

**JUSTIFICACION CONDICION " D "**

$$N + 1 = \frac{(a-3)^2}{4} + \frac{(a-1)^2}{4} + \frac{(a+1)^2}{4} + \frac{(a+3)^2}{4} + 16\, t(t+1)$$

$$t = \frac{b-2}{4}$$

---

$$N = a^2 + b^2 \quad ; \quad N \equiv -3 \pmod 8 \equiv 1 \pmod 4 \qquad a > 1 \qquad b > 1$$

Consideramos , " a " , el cuadrado impar $b \equiv 2 \pmod 4$

En base a lo expuesto en las condiciones anteriores ,

$$N = \frac{(a-3)^2}{4} + \frac{(a-1)^2}{4} + \frac{(a+1)^2}{4} + \frac{(a+3)^2}{4} + \frac{(b-6)^2}{4} + \frac{(b-2)^2}{4} + \frac{(b+2)^2}{4} + \frac{(b+6)^2}{4} - 25$$

sumamos a N , la unidad . El término independiente será - 24 .

La segunda parte de la ecuación , elevamos sus términos al cuadrado ,

$$\frac{b^2 - 12b + 36 + b^2 - 4b + 4 + b^2 + 4b + 4 + b^2 + 12b + 36 - 96}{4} = b^2 - 4$$

habíamos dicho, que $b \equiv 2 \pmod 4$ $b = 2 + 4t$

$$b^2 - 4 = (2 + 4t)^2 - 4 = 16t^2 + 16t = 16t(t+1)$$

$$N + 1 = \frac{(a-3)^2}{4} + \frac{(a-1)^2}{4} + \frac{(a+1)^2}{4} + \frac{(a+3)^2}{4} + 16t(t+1)$$

Luego tenemos como condición necesaria y suficiente , para que "N" sea igual a la suma de dos cuadrados , la arriba expuesta , es decir que " N + 1 " sea igual a la suma de 4 cuadrados consecutivos , más 16 veces el producto de dos determinados números consecutivos.

Ejemplo :

$$N = 15.993.157 = 3.999^2 + 34^2 \qquad t = \frac{34 - 2}{4} = 8$$

$$15.993.158 = 1.998^2 + 1.999^2 + 2.000^2 + 2.001^2 + 16 \quad (8 \times 9)$$

---

**BIBLIOGRAFIA**

(1) Morris Kleine.-El pensamiento matemático ,de la antigüedad a nuestros días (pag.367-368) (Alianza Universidad)

(2) Blas Torrecilla Jover.- Fermat,el mago de los números (pag.38 ) Editorial Nivola